ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

File Secured by Means of Dynamic Key Updation

Aruna Devi[1] , Anu Lekshmi[2], Deepak[3], Rama Lakshmi[4]

Assistant Professor, Department of CSE, RVS College of Engineering and Technology, Coimbatore, Tamil Nadu, India[1]

UG Student, Department of CSE, RVS College of Engineering and Technology, Coimbatore, Tamil Nadu, India[2,3,4]

ABSTRACT: Cloud security refers to a wide range of strategies and policies formulated to provide data applications and the cloud system applications. Cloud based applications are convenient for many businesses they enable secure data management, analysis and access from anywhere. Secure file transfer is data sharing via a secure, reliable delivery method. It is used to safeguard proprietary and personal data in transit and at rest. In this paper we introduce Dynamic Key updation to provide security to the file after downloading the file from cloud. The proposed protocol is demonstrated to resist against various attacks and also evaluate the performance of the proposed protocol with existing data sharing protocols. Also mutual authentication is provided without providing personal details of the customer.

KEYWORDS: cloud computing, Dynamic Key update, IBADS protocol, AVIPSA, Privacy protecting cloud

I. INTRODUCTION

Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use. Because of the clouds very nature as a shared resource, identity management, privacy and access control are of particular concern. With more organizations using cloud computing and associated cloud providers for data operations, proper security. In these and other potentially vulnerable areas have become a priority for organizations contracting with a cloud computing provider. cloud computing security process should address the security controls cloud provider will incorporate to maintain the customers data security, privacy and compliance with necessary regulations.

Identity based authentication protocol is used to provide data security in a cyber physical cloud environments. This protocol protect against various attacks. secure authentication between a physical device and a cloud controller is provided by Identity based encryption scheme and also secure end to end communication is provided by bilinear pairing. Automated Validation of Internet Security Protocol and Application ensures protection of security attacks against active and passive. This is an authentication protocol and automatically validate the attacks and provide security. Simulation of IBADS protocol using AVIPSA software is an authentication technique to check authorization of the client during logging into the cloud server.

Identity based encryption scheme is a cryptographic solution that can be used to facilitate secure data sharing. It is important primitive of ID based cryptography. In this scheme identity is taken as a public key. Encryption is done by using the public parameter and the master key.

Dynamic Key Update means updating dynamic sequence of keys. Dynamic keys are one-time symmetric cryptography keys forming sequence of keys. A dynamic key is used to produce sequence of dynamic keys from initial key parameters. The decisional strong Diffie-Hellman algorithm is used as the basis to prove the security of many cryptographic protocol. The decisional Diffie-Hellman assumption is a computational hardness assumption about a certain problem involving discrete logarithms in cyclic group.

II. LITERATURE REVIEW

In Supporting Heterogeneity in cyber-physical systems architecture the cyber- physical systems are heterogeneous which are traditionally considered separately. Here multi view architecture framework is proposed that treats models as

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

views of the underlying system structure and semantic mapping to ensure consistency and enable system level verification. This system treats cyber and physical elements equally well in a great fashion. But the behavior relations presented in this paper are mathematical definitions. This will be difficult for the user.

In Secure Scalable Document Sharing on Public cloud a novel architecture and corresponding protocols to provide secure sharing of documents on public cloud services. This system uses AES for Data encryption to achieve scalability and supports identity based access control rules using private public key pairs to provide flexibility. The drawback in this system is there is no secure password management system including the feasibility of password recovery.

In a survey of mobile computing application models, the cloud computing technology offers virtually unlimited dynamic resources for computation, storage and service provision by using partioning algorithms. So that mobile cloud execution platforms is standardized for ease computation. But the developed applications usually support one execution platform.

In security and privacy for health care networks, security and privacy protection in mobile health care networks from the quality of protection perspective is investigated which offers users adjustable security protection at fine grained levels. Here they overcame privacy leakage, misbehavior, and security in health data collection and processing by using recursive algorithms. But the mobile uses sometimes may not have tight social relationships with other in physical proximity. In Light weight static and dynamic attributes based access control, dynamic and static attributes are securely combined and developed novel access control technique. Here ABE scheme is used to reduce the computational complexity but it won't prevent junk information. The proposed scheme should not deny the illegal fog node's access request.

III. SYSTEM COMPOSITION

3.1 Software Components:

- ASP.Net
- C#.net
- MS SQL server

ASP.Net:

It is an open-source server-side web application framework designed for web development to produce dynamic web pages. It was developed by Microsoft to allow programmers to build dynamic web sites, web applications and web services. ASP.NET's successor is a ASP.NET core. It is re-implementation of ASP.NET as a modular web framework, together with other frameworks like Entity framework. The new framework uses the new open-source.NET compiler platform is cross platformASP.NET MVC, ASP.NET web API and ASP.NET web pages have merged into a unified MVC .It allows to use a full featured programming language such as C# or VB.NET to build web applications easily.

C # :

C# is an elegant and type-safe object-oriented language that enables developers to build a variety of secure and robust applications that run on the .NET framework. It is a simple, modern, general-purpose, object-oriented programming language developed by Microsoft within its .NET initiative led by Anders Hejlsberg. It is mainly used for developing desktop applications and more recently windows8/10 applications. It is an object oriented language and does not offer global variables or functions. C# is designed for Common Language Infrastucture.CLI is a specification that describes executable code and run time environment. C# automatically manages inaccessible object memory using a garbage collector, which eliminates developer concerns and memory leaks.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

MS SQL Server:

MS SQL server is a relational database management system developed by Microsoft. This product is built for the basic function of storing retrieving data as required by other applications. It can be run either on the same computer or on another across a network.SQL statements are used to perform tasks such as update data on a database.SQL server is a database server by Microsoft. It is a special-purpose programming language designed to handle data in a relational database management system. A database server is a computer program that provides database services to other programs or computers, as defined by the client-server model. As a database server, it is a software product with the primary function of storing and retrieving data as requested by other applications. Microsoft markets at least a dozen different editions of Microsoft SQL server, aimed at different audiences and for workloads ranging from small single-machine applications to large internet-facing applications with many concurrent users.SQL server also support for big data analytics and other advanced analytics applications through SQL server R services, which enables the DBMS to run analytics applications written in the open source R programming language.

IV. EXISTING SYSTEM

Despite the popularity of cloud computing and its variants, security issues in untrusted cloud environment and physical devices remain major concerns. In the existing system, Key generation is used. A single private key is stored to encrypt and downloading all the data's uploaded in the cloud. This may create security issue for the data consumer. Mutual authentication is provided by using the consumers personal details. Here there is chance of hacking by using the details of the consumer.

V. PROPOSED SYSTEM

In this paper Dynamic Key Updation strategy is introduced to frequently change private key after downloading the file from cloud. So this one increase the data consume security over the file. The mutual authentication is provided without providing consumers personal details. The proposed protocol will overcome the various security challenges such as Mutual Authentication, Password protection and impersonation resilience and it also ensures user anonymity. It act as resilience against various attacks such as insider attack, impersonation attack, session key computation attack, Android Mobstby and its correctness using AVIPSA simulation tool. The AVISPA protocol automatically validate the attacks and provide security. The physical devices are authenticated and secure end-to-end communication is provided.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

VI. MODEL DESCRIPTION

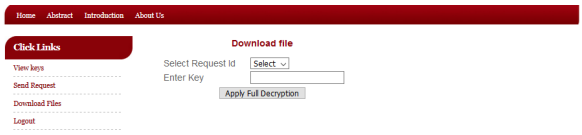
A. Encryption Of File:

The cloud service provider has to login into the page. Then data owner, data consumer and the public key generator has to be registered and authorized. After that the keys has to be set by PKG for the particular consumer and for the file. Then the file has to be encrypted by using the key generated by the PKG and has to be uploaded.

After uploading will receive a notification as given below,

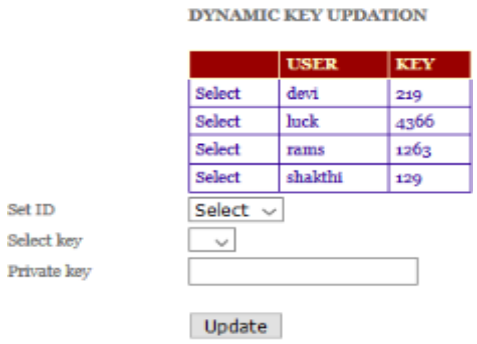
B. Decryption of File:

The data consumer has to login into the page. The data consumer has to get the private key of the file then only they can download and decrypt the file. To get the private key the consumer have to request the key to PKG. Only after getting mutual authentication, the PKG will display the key to the consumer, After the key is displayed, file can be downloaded and decrypted with that private key by the consumer.



C. Dynamic Key Updation:

After the file is downloaded by the consumer, the key will be frequently changed by using 'Dynamic key update' method to prevent the file from being hacked.



ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

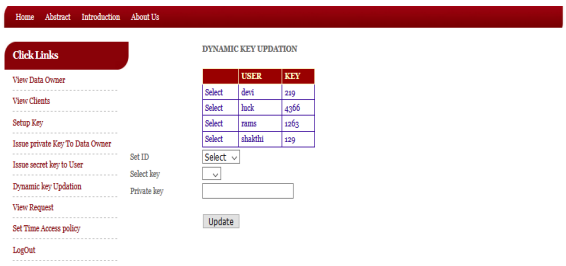
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

VI. IMPLEMENTATION RESULT

Dynamic Key update is provided for data consumers. The private key of the file will be frequently updated. So that the file is secured and cannot be hacked easily.



VII. CONCLUSION & FUTURE WORK

Henceforth, Dynamic Key Updation' is introduced to frequently change private key after downloading the file from cloud. So this one increase the data consume security over the file. In future research, intend to implement a prototype of the proposed protocol so that can evaluate its practicability in a real-world setting

REFERENCES

1. Akshay Rajhans and Bruce H.Krogh, "Supporting Heterogeneity in Cyber-Physical Systems Architectures", IEEE Transactions on automatic control, 2014.
2. Catherine Wise, Carsten Friedrich, "CloudDocs: Secure Scalable Document Sharing on Public Clouds", 2015 IEEE International conference on cloud computing.
3. Dijiang Huang and Yunji Zhong, Secure Data Processing Framework for Mobile Cloud Computing.
4. Zhi-Hua Zhang and Wei Jiang, "An Identity-Based Authentication Scheme in Cloud Computing", 2012 International conference on industrial control and Electronic engineering.